EXHIBIT 3
PUBLIC VERSION

Jill F. Kopeikin, State Bar No. 160792
Valerie M. Wagner, State Bar No. 173146
GCA LAW PARTNERS LLP
1891 Landings Drive
Mountain View CA 94043

Vincent E. McGeary, *Pro Hac Vice*
New Jersey State Bar No. 041681991
GIBBONS P.C.
One Riverfront Plaza
Newark, NJ
Phone: (973) 596-4837
Facsimile: (973) 639-6477
Email: vmcgeary@gibbonslaw.com

Michael Cukor, *Pro Hac Vice*
New York State Bar No. 3935889
GIBBONS P.C.
One Pennsylvania Plaza, 37th Floor
New York, New York 10119-3701
(212) 613-2013 (telephone)
(212) 554-9658 (facsimile)
Email: mcukor@gibbonslaw.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

Network Protection Sciences, LLC,

Plaintiff,

vs.

Fortinet, Inc.

Defendant.

Case No. 3:12-cv-01106-WHA

NETWORK PROTECTION SCIENCES, LLC'S UPDATED ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS (PATENT L. R. 3-1); AND ACCOMPANYING DOCUMENT PRODUCTION (PATENT L. R. 3-2)

JURY TRIAL DEMANDED

Pursuant to the Court's June 20th, 2012 Case Management Order (Dkt No. 153) and Patent Local Rules 3-1 and 3-2 for the Northern District of California, Plaintiff Network Protection Sciences, LLC ("**NPS**") submits the following updated Asserted Claims and Infringement Contentions, and provides the accompanying document production to Defendant Fortinet, Inc. ("**Fortinet**").

I. DISCLOSURE OF UPDATED ASSERTED CLAIMSAND INFRINGEMENT CONTENTIONS.

NPS's investigation is ongoing, and NPS expects to receive documents from Fortinet likely to be highly relevant to NPS's claims of infringement and the disclosures and contentions set forth herein. NPS therefore reserves the right to amend, modify, supplement or revise these disclosures, including additional accused instrumentalities as defined in Patent Local Rule 3-1(b) after Defendant complies with its discovery obligations and documents are produced, depositions taken, additional facts are ascertained, and analyses made, or as a result of the Court's determination of issues.

Nothing in these contentions is intended to be nor should be construed as a waiver of the attorney-client privilege or work attorney work product doctrine.

A. Patent Local Rule 3-1(a)—Updated Asserted Claims.

NPS currently asserts that Fortinet is liable under 35 U.S.C. § 271(a), (b), and (c) for infringing U.S. Patent No. 5,623,601 ("the '**601** patent). Specifically, NPS alleges that Fortinet infringes claims 1-25, 28-53, and 55-57 of the '601 patent (the "**Asserted Claims**").

B. Patent Local Rule 3-1(b)—Updated Accused Instrumentalities.

The Accused Instrumentalities include secure gateways employing the FortiOS platform such as those identified in **Exhibit B**. The Accused Instrumentalities include methods which are embodied in executable instructions and these infringement contentions extend to all Fortinet products executing such methods. Defendant Fortinet directly and/or indirectly infringes and/or contributes to and/or induces the infringement of the Asserted Claims by making, selling, distributing, and causing its customers to use, product families, such as those identified in **Exhibit B** (many of which can be found within NPS's documents bates numbered NPS0050203-NPS0050766), that employ the FortiOS platform and are configurable, and have been configured, to implement a transparent application layer IP proxy server.

C. Patent Local Rule 3-1(c)—Updated Claim Chart for the Accused Instrumentalities.

Exhibit A identifies where each element of each Asserted Claim is found in the Accused Instrumentalities. The Accused Instrumentalities use the FortiOS platform and thus the infringement chart in **Exhibit A** applies to all products identified in **Exhibit B** and other products carrying out or configurable to carry out the functionality identified in the FortiOS platform. The identified source code evidence is exemplary for proxies imd and http. FortiOS implement proxies such as ftp, imap, pop3, smtp, nntp, and ssl, in like manner, and these proxies correspond to the identified claim limitations for the same reasons identified for the imd and http proxies. These contentions extend to all proxies implemented in like manner, whether or not Fortinet has provided such source code or whether such source code has been specifically identified. Further, also provided is exemplary source code for virtual server daemon and wireless optimization daemon; it is NPS's position that any Fortinet products using other equivalent functionality would infringe as well.

Additionally, NPS has provided citations to Fortinet technical literature, and will rely upon the Fortinet FortiOS Handbook v2 and information in subsequent handbooks, including versions 2.5, 2.8, 3.0, and 4.0 found at http://docs.fortinet.com/fgt.html.

D. Patent Local Rule 3-1(d)—Updated Indirect Infringement.

In addition to the direct infringement perpetuated by Fortinet, Fortinet also actively contributes to and induces infringement. Fortinet—in violation of 35 U.S.C. § 271(b)—has knowingly induced infringement and possessed specific intent to encourage another's infringement of one or more claims of the '601 patent by, among other things, making, selling, distributing, and causing its customers to use, product families that include a transparent IP proxy server such as, without limitation, the FortiGate products, to certain companies as shown further below. Also, Fortinet induces infringement *e.g.* through users of the Fortinet products or Fortinet users with network users.

Additionally, in violation of 35 U.S.C. § 271(c), Fortinet has contributorily infringed and continues to contributorily infringe to the same companies as shown further below, by: (a) selling and/or offering to sell within the United States the FortiGate products within its own products and services; (b) integrating the FortiGate products within the companies' products to constitute a material part of the invention of the '601 patent; (c) knowing that the FortiGate products are to be especially adapted for use in infringing the '601 patent; and (d) failing to develop the Fortinet products as suitable for substantial noninfringing use with respect to the '601 patent. The products implementing the FortiOS platform are specially adapted to execute the Accused Intsrumentality, including the identified transparent proxy servers. Fortinet FortiOS Handbook describes and teaches users to implement the Accused Instrumentality.

An example of Fortinet's induced and contributory infringement is the use by Guess? Inc. ("Guess") of the FortiGate products . *See* NPS0050069-70. Upon information and belief Guess has replaced SonicWALL products with FortiGate products at all 500 of its stores in North America and its corporate headquarters in Los Angeles, California, thereby ensuring that Guess will use the FortiGate products. Fortinet has issued a press release announcing this replacement so Fortinet's customers, including Guess, would be aware of Guess's use of the FortiGate products. The following are excerpts from Fortinet's press release:

> . . . . Guess?, Inc., a $2 billion retail company with more than 800 locations throughout the world, has selected Fortinet appliances over competitive appliances, such as Juniper . . . and SonicWall, to provide firewall, IPSec VPN, intrusion prevention.
> . . . .
> 'We were looking for a network security solution that could replace our previous vendors and, in the process, we got a lot more than what we paid for with Fortinet's scalable, multifunction appliances . . . . The Fortinet solution has enabled us to manage all our North American stores with a single pane of glass while easing the burden of management, configuration and deployment for so many remote locations.'
>
> The first part of the Fortinet deployment consisted of replacing SonicWall appliances at all 500 U.S. and Canadian retail stores. The FortiGate®-60C, FortiGate-200B and FortiGate-310B appliances are now deployed throughout the store network and are helping provide firewall, VPN, Web content filtering and 3G failover for the stores.
>
> The second part of the deployment consisted of replacing its previous Cisco solution at the Guess? datacenter. Two FortiGate-1240B appliances are located at the datacenter and helping provide firewall protection and IPSec VPN connectivity. In addition, to manage the network traffic of all the stores, a FortiManager™-3000C appliance has been deployed at the datacenter.
>
> The third part of the Guess? deployment of FortiGate appliances was at the corporate headquarters located in Los Angeles. Two FortiGate-310B appliances deployed in active/passive mode are being used for the corporate firewall and VPN as well as Web content filtering.

NPS0050069 (emphasis added).

Similarly, like Guess, Siemens Enterprise Communications, Inc. ("Siemens") is using the Fortient products. A Fortinet a press release announcing Siemens using the FortiGate products is states: "While Siemens Enterprise Communications already fully exploits all the extensive functions of Fortinet's UTM solutions for its customers within the data area, the provider primarily uses the FortiGate firewall and IPS features for its OpenScape secure cloud services." NPS0050072. Additionally

> Communication projects frequently involve the deployment of a 'UC Firewall', depending on the project size and the customer environment. Siemens Enterprise Communications requested high performance design of their UC firewall solution, which is based on three Fortinet's hardware platforms: The FortiGate-310B, the FortiGate-620B and the FortiGate-1240B network security appliances. With all FortiGate models (from the FortiGate-200B upwards) being compatible and suitable for this application, Siemens Enterprise Communications can provide the right solution to meet every architecture requirement, irrespective of the size of the customer or project.
>
> . . . .
>
> The Fortinet appliances allow the secure integration of Siemens Enterprise Communications solutions into a customer mixed infrastructure, with the new UC firewall solution equally supporting data application, voice and UC traffic.
>
> . . . .
>
> 'With the new highly available and failure-resistant clusters, we satisfy the cloud service high standards that our customers expect. Confidentiality and reliability are not important to our customers only. We also expect our partners to respond quickly and efficiently when it comes to solving problems.'
>
> . . . .
>
> 'The outstanding price performance ratio offered by Fortinet was also a decisive factor, since Fortinet enables us to offer the right security solution at a competitive price, according to the customer, project size and security requirements' . . . .

Id. (emphasis added).

Others are similarly using FortiGate products and thus make Fortinet liable for induced and contributory infringement under 35 U.S.C. §§ 271(b) and (c), such as MegaPath (*See* NPS0050073; NPS0050077 (contains Fortinet confidential information)), BAI Security (*See* NPS0050073), Nuspire (*See* NPS0050073), LockNET (*See* NPS0050073), Unisys (*See* NPS0050078 (contains Fortinet confidential information)), Polycom (*See* NPS0050084-87), VMware (*See* NPS0050088-89), Honda/Colliers International/Ryserson University/Pierre

Lang/Pizza Hut (*See* NPS0050090), Tech Data Corporation (*See* NPS0050092-95), Abington Public Schools (*See* NPS0050096-97), Jefferson County (*See* NPS0050098-99), Northwest Independent School (*See* NPS0050100-101), State of Nebraska (*See* NPS0050102-103), State of South Dakota (*See* NPS0050104-105), Accuity (*See* NPS0050106-107), American Axle & Manufacturing (*See* NPS0050108-109), BHI Advanced Internet (*See* NPS0050110-112), DJO (*See* NPS0050113-115), Frederick Innovative Technology Center (*See* NPS0050116-118), Freedom Health (*See* NPS0050119-120), Global Crossing (*See* NPS0050121-122), Green Mountain Access (*See* NPS0050123-124), Harley-Davidson (*See* NPS0050125-126), Panda Restaurant Group (*See* NPS0050127-128), Paradigm Investment Group (*See* NPS0050129-130), PSC Info. Group (*See* NPS0050131-132), Qdoba Mexican Grill (*See* NPS0050047-48), Roche Brothers (*See* NPS0050049-50), Rural Wisconsin Healthcare Cooperative (*See* NPS0050051-52), SmartBusiness (*See* NPS0050053-55), SoftLayer (*See* NPS0050056-57), Terenine Technology Solutions (*See* NPS0050058-59), Troon Golf (*See* NPS0050060-61), Valvoline Instant Oil Change (*See* NPS0050062-64), Verizon Business (*See* NPS0050064-66), and Whyte Hirschboeck Dudek S.C. (*See* NPS0050067-68).

The preceding are evidentiary examples of acts of indirect infringement of which NPS is aware of, and NPS reserves the right to supplement upon receiving additional information.

E. Patent Local Rule 3-1(e)—Nature of Infringement.

The infringement chart attached as **Exhibit A** outlines which elements are present literally and/or under the doctrine of equivalents.

F. Patent Local Rule 3-1(f)—Priority Date.

All asserted claims of the ‘601 patent are entitled to the priority date of the filing date of the ‘601 patent.

G. Patent Local Rule 3-1(g)—Patentee’s Asserted Practice of the Claimed Inventions.

None.

H. Patent Local Rule 3-1(h)—Willful Infringement.

Fortinet has willfully infringed the '601 patent. On information and belief, Fortinet had knowledge of the '601 patent since it issued, as Michael Xie, the founder and Chief Technical Officer of Fortinet, was a Senior Software Engineer at Milkyway Networks Corporation, the assignee of the '601 patent at the time it issued. *See* NPS0050160-61.

Additionally, Fortinet had knowledge of the '601 patent through one of its former engineers, Mr. Jin Shang (http://www.linkedin.com/pub/jin-shang/12/306/136) Mr. Shang was an inventor of U.S. Patent 7,996,894 which cited the '601 patent as prior art on February 15th, 2005; this is the very same time that he was an engineer at Fortinet. (*See* U.S. Patent 7,996,894, Information Disclosure Statement, dated February 15, 2005; *and see* Linkedin profile of Jin Shang: http://www.linkedin.com/pub/jin-shang/12/306/136.) Of note Mr. Shang is also a coinventor of U.S. Patent 7,606,225 with Mr. Michael Xie who as described above worked at Milkyway Networks Corp.

Notwithstanding knowledge of the '601 patent, and with recklessness, Fortinet continues to infringe the '601 patent.

II. DOCUMENT PRODUCTION ACCOMPANYING DISCLOSURES[1]

In conformance with Patent Local Rule 3-2,NPS responds as follows: Copies of the documents required for Patent Local Rule 3-2(a)-(e) are listed in the below table.

Local Patent Rule	Bates Range Location
3-2(a) (pre-application disclosure)	NPS0000358-360.
3-2(b) (conception and reduction to practice)	NPS0000020 - NPS0000357 and NPS0000358 - NPS0000368.
3-2(c) (file histories)	NPS0000020 - NPS0000357
3-2(d) (ownership)	NPS0050164-NPS0050201.
3-2(e) (asserted practice of claimed inventions)	None

[1] As Patent Local Rule 3-2(a) states, "A party's production of a document as required herein shall not constitute an admission that such document evidences or is prior art under 35 U.S.C. § 102."

This response is subject to the limitations and reservations set forth above, and in particular includes Plaintiff's objection to the production of information protected by the attorney-client privilege or which is protected by the attorney work product doctrine, or other applicable privileges, and is based upon the information presently available to Fortinet. These contentions are being e-mailed to counsel for Fortinet at Wilson Sonsini Goodrich and Rosati on August 31, 2012, and the accompanying production (NPS0050047 - NPS0050766) is being made in electronic format for overnight delivery.

Certain of these materials are being produced with a designation of "HIGHLY CONFIDENTIAL – ATTORNEYS EYES ONLY" of "HIGHLY CONFIDENTIAL - SOURCE CODE" pursuant to the Protective Order entered (Dkt No. 160) as amended (Dkt No. 161) in this case.

GCA LAW PARTNERS LLP

DATED: August 31, 2012

By: /s/ Jill F. Kopeikin
Jill F. Kopeikin
Valerie M. Wagner
GCA LAW PARTNERS LLP
1891 Landings Drive
Mountain View CA 94043
California State Bar #160792

CERTIFICATE OF SERVICE

I declare that I am employed with the law firm of **GCA LAW PARTNERS LLP**, whose address is 1891 Landings Drive Mountain View CA 94043. I am not a party to the within cause, and I am over the age of eighteen years.

I further declare that on August 31, 2012, I served a copy of:

NETWORK PROTECTION SCIENCES, LLC'S UPDATED ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS (PATENT L. R. 3-1); AND ACCOMPANYING DOCUMENT PRODUCTION (PATENT L. R. 3-2)

by electronically mailing a true and correct copy through GCA LAW PARTNERS LLP's electronic mail system to the e-mail address(es) set forth below, or as stated on the attached service list per agreement in accordance with Federal Rules of Civil Procedure rule 5(b):

STEFANI E. SHANBERG (Cal. Bar No. 206717)
ROBIN L. BREWER (Cal. Bar No. 253686)
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, California 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100
E-Mail: sshanberg@wsgr.com
rbrewer@wsgr.com

Attorneys for Defendant FORTINET, INC.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at Mountain View, California this 31st day of August, 2012.

EXHIBIT A

INFRINGEMENT CHART FOR THE 5,623,601 PATENT

The infringement evidence cited below is exemplary and not exhaustive. The cited examples are taken from source code produced by Fortinet and other Fortinet technical documentation. NPS's infringement contentions apply to all Fortinet products incorporating FortiOS having the same or similar functionality, including past and expected future releases. NPS reserves the right to rely upon all admissible evidence to prove its allegations of infringement.

The exemplary source code referenced in the infringement contentions below is provided for proxies imd and http, or as may be indicated. FortiOS also implements ftp, imap, pop3, smtp, nntp, and ssl, in the same manner, and such implementations also infringe and are part of these contentions. Further, also cited below is exemplary source code for virtual server daemon and wireless optimization daemon; it is NPS's position that any Fortinet products using other equivalent functionality would infringe as well.

Additionally, where NPS cites to Fortinet documentation, such as the Fortinet FortiOS Handbook v2, NPS relies upon the same or similar functional descriptions in other Fortinet documents, including versions 2.5, 2.8, 3.0, and 4.0 found at http://docs.fortinet.com/fgt.html.

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
1. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	If any claim preamble is determined to recite a limitation, then plaintiff states literal or equivalent for all preambles.
(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path	A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
to the host, but encapsulating the packets with a hardware destination address that matches a device address of the gateway;	*FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	
(b) accepting at the gateway communications packets from either network that are encapsulated with a hardware destination address which matches the device address of the gateway;	The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	L
(c) determining at the gateway whether there is a process bound to a destination port number of an accepted communications packet;	FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231, P. 191, P. 196-197* FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported and are within these contentions. The below redirect code is exemplary and works the same or similarly for all proxies. *FortiGate Version 4.0 MR2 Administration Guide P.220- 226*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] FORTINET-NPS-SC 000035-000036 [803:804] [redacted] [808:856] [redacted] [redacted] FORTINET-NPS-SC 000043 [3:14] [redacted] [redacted] FORTINET-NPS-SC 000039-000043 [9:16] [redacted] [124:126] [redacted] [redacted] FORTINET-NPS-SC 000037-000038 [4:5] [redacted] [redacted] FORTINET-NPS-SC 000066-000074 [58:67]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] **FORTINET-NPS-SC 000110-000114** **[1711:1716]** [redacted]	
(d) establishing transparently at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;	If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established (as indicated by creating an entry in the session table), else the packet is dropped. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff* FortiWeb Data Sheet, P1 [redacted] **FORTINET-NPS-SC 000066-000074** **[4:9]** [redacted] **[196:200]** [redacted] **fortinet\proxy\imd\imd_session.h** **FORTINET-NPS-SC 000119-000124** **[37:41]** [redacted]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] **FORTINET-NPS-SC 000115-000116** **[36:69]** [redacted] [redacted] **FORTINET-NPS-SC 000117-000118** **[22:51]** [redacted] **relevant:** [redacted] **FORTINET-NPS-SC 000109**	
(e) establishing transparently at the gateway a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and	Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet. "Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions." The imd and http proxies outlined below are exemplary and this applies to all other proxies, such ftp, imap, pop3, smtp, nntp, and ssl. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff, P.*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	186-187 [redacted] **FORTINET-NPS-SC 000066-000074** **[196:200]** [redacted] [redacted] **FORTINET-NPS-SC 000058-000063** **[1158:1422]** [redacted] **same for:** [redacted] **FORTINET-NPS-SC 000119-000124** **[43:48]** [redacted] [redacted] **FORTINET-NPS-SC 000110-000114** **[59:63]**	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [1711:1719] [redacted] [redacted] FORTINET-NPS-SC 000140-000145 [1456:1476] [redacted] [3190:3194] [redacted] relevant: [redacted] FORTINET-NPS-SC 000109	
(f) transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the	Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.* [redacted] FORTINET-NPS-SC 000066-000074 [201:204]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
source and the second session communicates with the destination using the data moved between the first and second sessions.	[redacted] [269:275] [redacted] [redacted] FORTINET-NPS-SC 000119-000124 [50:54] [redacted] [250:258] [redacted] [redacted] FORTINET-NPS-SC 000075-000077 [32:96] [redacted] [redacted] FORTINET-NPS-SC 000140-000145 [3997:4013] [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] [redacted] FORTINET-NPS-SC 000064-000065 [862:867] [redacted] [redacted] FORTINET-NPS-SC 000015-000034 [4:5] [redacted] [24:25] [redacted] [843:864] [redacted]	
2. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the step of determining involves checking to determine if a process is bound to the	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." Policies need not be bound to a specific destination port, or service. Generic policies may be defined to cover TCP packets or UDP packets destined for any port or range of ports.	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
destination port number, and passing the packet to a generic process if a process is not bound to the destination port number, the generic process acting to establish the first and second communications sessions and to move the data between the first and second communications sessions.	http://www.fortinet.com/products/fortigate/ *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 226, 215* [redacted] **FORTINET-NPS-SC 000066-000074** **[206:209]** [redacted] [redacted] **FORTINET-NPS-SC 000015-000034** **[4:22]** [redacted] [redacted] **FORTINET-NPS-SC 000132** **[8:19]** [redacted] [redacted] **FORTINET-NPS-SC 000133** **[3967:3987]**	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] FORTINET-NPS-SC 000134-000136 [119:122] [redacted] fortinet\daemon\wad\wad_app_mgr.c FORTINET-NPS-SC 000146 [6:13] [redacted] [redacted] FORTINET-NPS-SC 000147-000150 [105:114] [redacted] [redacted] FORTINET-NPS-SC 000151 [9:16] [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted]	
3. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) checking a rule base to determine if the source address requires authentication; and	The list of policies includes identity-based policies which require authentication based on source address. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 925, 975-979* [redacted] **FORTINET-NPS-SC 000078-000082** **[5:14]** [redacted]	L/E
b) authenticating the source by requesting a user identification and a password and referencing a database to determine if the user identification and password are valid.	FortiOS authenticates with a user identification and password checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* [redacted] **FORTINET-NPS-SC 000078-000082** **[15:19]** [redacted]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] **FORTINET-NPS-SC 000083-000096** **[443:444]** [redacted] **[463:464]** [redacted] **[603:615]** [redacted] [redacted] **FORTINET-NPS-SC 000098-00009** **[17:18]** [redacted] **[50]** [redacted]	
4. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) referencing a rule base after the first communications session is established	A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether the	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
to determine whether the source address is permitted access to the destination address for a requested type of service; and	communication is permitted. The ability to add rules and/or policies is exemplary and applies to any rules or policies used. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.189* [redacted] **FORTINET-NPS-SC 000078-000082** **[151:154]** [redacted]	
b) cancelling the first communications session if the rule base does not include a rule to permit the source address to access the destination address for the requested type of service.	If a policy does not permit a packet, the packet is denied. The first communication session is cancelled. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.189* [redacted] **FORTINET-NPS-SC 000078-000082** **[151:156]** [redacted]	L/E
5. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 3, wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 3. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and	Once a user successfully authenticates, the FortiGate security device creates an entry in the authentication table for the user's IP address. *FortiOS™ Handbook v2: User Authentication, P.47* [redacted] **FORTINET-NPS-SC 000078-000082** **[151:156]** [redacted]	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted]	
b) referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source.	FortiOS devices provide authentication timeout. A user need not authenticate again during the timeout period. This authentication table (and check to see if any change has occurred) is exemplary and applies to any Fortinet product which gives the ability to remember when a source address was previously authenticated. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923* [redacted] **FORTINET-NPS-SC 000078-000082** **[179:183]** [redacted]	E
6. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 5 wherein the user authentication file includes a creation time variable which is set to a system time value when the user is authenticated.	We incorporate here the evidence cited in support of claim 5. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000107-00108** **[53:75]** [redacted] [redacted] **FORTINET-NPS-SC 000100-00106** **[130:269]** [redacted]	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted]	
7. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 6 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 6. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) updating a modification time variable of the authentication file each time the user initiates a new communications session through the gateway station.	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 899,902,* [redacted] **FORTINET-NPS-SC 000107-00108** **[741:773]** [redacted]	E
8. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 7 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 7. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) periodically checking each user authentication file to	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and	authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902* [redacted] **FORTINET-NPS-SC 000107-00108** **[775:789]** [redacted]	
b) deleting the user file from the user authentication directory if the threshold has been exceeded by each of the first and second differences.	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902* [redacted] **FORTINET-NPS-SC 000078-000082** **[15:21]** [redacted] **[181:183]** [redacted]	E
9. A method for providing a secure gateway between a private network and potentially hostile network as claimed in claim 1 wherein the method further	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	.

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
involves the steps of:		
a) performing a data sensitivity check on the data associated with each packet as a step in the process of moving the data between the respective first and second communications sessions.	FortiGate security devices implement UTM components which perform data sensitivity checking while transferring data. The below is an exemplary data sensitivity check and applies to all data sensitivity checks done in Fortinet source code. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Chapter 6* [redacted] **FORTINET-NPS-SC 000125-000126** **[5:8]** [redacted] [redacted] **FORTINET-NPS-SC 000127** **[8:11]** [redacted] [redacted] **FORTINET-NPS-SC 000128** **[11:35]** [redacted] [redacted] **FORTINET-NPS-SC 000129-000130** **[11]** [redacted] [redacted] **FORTINET-NPS-SC 000131** **[8:13]**	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] **FORTINET-NPS-SC 000044-000045** **[10:18]** [redacted] **http://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol** The Internet Content Adaptation Protocol (ICAP) is a lightweight HTTP-like protocol specified in RFC 3507 which is used to extend transparent proxy servers, thereby freeing up resources and standardizing the way in which new features are implemented. ICAP is generally used to implement virus scanning and content filters (including censorware) in transparent HTTP proxy caches.	
10. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to host, but encapsulating the packets with a hardware destination address that matches a device address of the gateway;	A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
(b) accepting from either network all TCP/IP packets that are encapsulated with a hardware destination address which matches the device address of the gateway;	The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185*	L
(c) determining whether there is a proxy process bound to a port for serving a destination port number of an accepted TCP/IP packet;	FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* FortiWeb Data Sheet, P1 FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported by using Application Layer Proxies. *FortiGate Version 4.0 MR2 Administration Guide P.220- 226* [redacted] **FORTINET-NPS-SC 000039-000043** **[41:45]** [redacted] We incorporate here the evidence cited in support of claim 1c.	L/E
(d) establishing a first communications session with a source address/source port number of the accepted TCP/IP packet if there	If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is established as indicated by creating an entry in the session table, else the packet is dropped. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff*	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
is proxy process bound to the port for serving the destination port number, else dropping the packet;	FortiWeb Data Sheet, P1 We incorporate here the evidence cited in support of claim 1d.	
(e) determining if the source address/source port number of the accepted packet is permitted to communicate with a destination address/destination port number of the accepted packet by referencing a rule base, and dropping the packet if a permission rule cannot be located;	FortiOS determines whether a packet is permitted to communicate with a destination address/port number of an accepted communications packet by matching the packet to a policy in the policy rule base and drops the packet if there is no match: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* We incorporate here the evidence cited in support of claim 4a and 4b.	L/E
(f) establishing a second communications session with the destination address/destination port number of the accepted TCP/IP packet if a first communications session is established and the permission rule is located; and	Depending on the action(s) determined by policy and the first communications session, the session table is updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet. "Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff* We incorporate here the evidence cited in support of claim 1e.	L
(g) transparently moving data associated with each subsequent TCP/IP packet between the respective first and second communications	Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189,*	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.	*Chapter 6.* We incorporate here the evidence cited in support of claim 1f.	
11. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10 wherein the step of determining involves checking a table to determine if a custom proxy process is bound to the destination port number, and passing the packet to a generic proxy process if a custom proxy process is not bound to the destination port number, the generic proxy process being executed to establish the first and second communications sessions and to move the data between the first and second communications sessions.	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." Policies need not be bound to a specific destination port, or service. Generic policies may be defined to cover TCP packets or UDP packets destined for any port or range of ports. http://www.fortinet.com/products/fortigate/ *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 226* We incorporate here the evidence cited in support of claim 2.	L/E
12. A method of providing a secure gateway between a	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
private network and a potentially hostile network as claimed in claim 10 wherein the step of establishing a first communications session with a source address/source port number further involves the steps of:	between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) checking a rule base to determine if the source requires authentication;	The list of policies includes identity-based policies which require authentication based on source address. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 925* We incorporate here the evidence cited in support of claim 3a.	L/E
b) checking an authentication directory to determine if an authentication file exists for the source in an instance where the source requires authentication; and	Once a user successfully authenticates, the FortiGate security device creates an entry in the authentication table for the user's IP address. *FortiOS™ Handbook v2: User Authentication, P.47* We incorporate here the evidence cited in support of claim 5a.	L/E
c) if the source requires authentication and an authentication file for the source cannot be located, authenticating the source by requesting a user identification and a password and referencing a user identification database to determine if the user identification and password are valid.	FortiOS authenticates with a user identification and password if no entry exists in the authentication table that checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* We incorporate here the evidence cited in support of claim 3b.	L

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
13. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 12 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 12. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) referencing a rule base as a first step after the first communications session is established to determine whether the user identification/password at the source address is permitted to communicate with the destination address for a requested service; and	A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether the communication is permitted. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.189* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.925-927* We incorporate here the evidence cited in support of claim 3b and 4a.	L/E
b) cancelling the first communications session if the rule base does not include a rule to permit the user identification/password at the source address to communicate with the destination address for the requested type of service.	If a policy does not permit a packet, the packet is denied. The first communication session is cancelled. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923* We incorporate here the evidence cited in support of claim 4b.	L/E
14. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in	We incorporate here the evidence cited in support of claim 12. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/*	

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
claim 12, wherein the method further involves the steps of:	*Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and	Once a user successfully authenticates, the FortiGate security device creates an entry in the authentication table for the user's IP address. *FortiOS™ Handbook v2: User Authentication, P.47* Once a user authenticates using one of the defined protocols, they can access any resource permitted by the identity policy. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 925-927* We incorporate here the evidence cited in support of claim 5a.	L/E
b) referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source having an authentication file in the authentication directory.	Once a user authenticates using one of the defined protocols, they can access any resource permitted by the identity policy. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 925-927* FortiOS devices provide authentication timeout. A user need not authenticate again during the timeout period. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923* We incorporate here the evidence cited in support of claim 5b.	L/E
15. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 14 wherein a file creation time variable which is automatically set by an operating system of the gateway station to a system	We incorporate here the evidence cited in support of claims 6a and 14.	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
time value when a file is created, is used to monitor a time when the user is authenticated.		
16. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 14 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 14. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	.
a) rewriting the user authentication file each time the user initiates a new communications session through the gateway station so that a modification time variable in the authentication file is automatically updated by the operating system of the secure gateway.	We incorporate here the evidence cited in support of claim 7a.	E
17. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 16 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 16. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) periodically checking each user authentication file to	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and	authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.902* We incorporate here the evidence cited in support of claim 8a.	
b) deleting the user file from the user authentication directory if the threshold has been exceeded by both of the first and second differences.	We incorporate here the evidence cited in support of claim 8b.	E
18. A method for providing a secure gateway between a private network and potentially hostile network as claimed in claim 10 wherein the method further involves the steps of:	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) performing a data sensitivity check on the data portion of each packet as a step in the process of moving the data between the respective first and second communications sessions, whereby the	FortiGate security devices implement UTM components which perform data sensitivity checking while transferring data. These content inspection functions are performed by proxies, including the AV proxy. The proxies inspect the packet data before sending the packet data to the destination via the second communication session, thereby operating at the application layer. The UTM components receive the data from the FortiOS which is a modified operating system kernel. The UTM components implement screening algorithms. The data sensitivity checking operates on	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
TCP/IP packet is passed by a modified kernel of an operating system of the secure gateway to the proxy process which extracts the data from the packet and passes the data from a one of the first and second communications sessions to a proxy process which operates at an application layer of the gateway station and the proxy process executes data screening algorithms to screen the data for elements that could represent a potential security breach before the data is passed to the other of the first and second communications sessions.	TCP/IP protocols. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Chapter 6* We incorporate here the evidence cited in support of claim 9a.	
19. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network, comprising in combination:	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* We incorporate here the evidence cited in support of claim 1.	
a gateway station adapted for connection to a telecommunications connection with each	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184,*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
of the private network and the potentially hostile network;	*185* We incorporate here the evidence cited in support of claim 1.	
an operating system executable by the gateway station, a kernel of the operating system having been modified so that the operating system:	FortiOS is an operating system executable at the FortiGate gateways. The kernel has been modified so that FortiOS: http://www.fortinet.com/products/fortigate/ Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185 http://gpl-violations.org/news/20050414-fortinet-injunction.html We incorporate here the evidence cited in support of claim 1.	L
a) cannot forward any communications packet from the private network to the potentially hostile network or from the potentially hostile network to the private network; and	The FortiOS kernel is modified so that packets with a destination IP address other than the gateway are not forwarded from the private network to the potentially hostile network or from the potentially hostile network to the private network without processing by the gateway. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173*	L/E
b) will accept for processing any communications packet from either of the private network and the potentially hostile network provided that the packet is encapsulated with a hardware destination address that matches the device address of the gateway station on the respective network; and	A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol* The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	We incorporate here the evidence cited in support of claim 1a.	
at least one proxy process executable by the gateway station, the at least one proxy process being adapted to transparently initiate a first communications session with a source of an initial data packet accepted by the operating system and to transparently initiate a second communications session with a destination of the packet without intervention by the source, and to transparently pass the data portion of packets received by the first communications session to the second communications session and to pass the data portion of packets received by the second communications session to the first communications session, whereby the first session communicates with the source using data from the second session and the second session communicates with the destination using data received from the first	FortiGate devices execute numerous proxy processes. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, generally and P. 193ff, Chapter 6* FortiWeb Data Sheet, P1 FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported by using Application Layer Proxies. *FortiGate Version 4.0 MR2 Administration Guide P.220- 226* During ingress processing, a first communications session is transparently established as shown by creating an entry in the session table). *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff* FortiWeb Data Sheet, P1 The session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet, without intervention from the source. "Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff, Chapter 6* Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189,*	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
session.	*Chapter 6* We incorporate here the evidence cited in support of claim 1c, 1d, 1e, and 1f.	
20. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the operating system is a Unix operating system.	We incorporate here the evidence cited in support of claim 19. FortiOS utilizes a modified Linux kernel. Linux is a Unix-like operating system. [redacted] **FORTINET-NPS-SC 000035-000036** **[803:804]** [redacted] We incorporate here the evidence cited in support of claim 1a.	E
21. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process includes modified public domain proxy processes for servicing Telnet, FTP, and UDP communications.	We incorporate here the evidence cited in support of claim 19. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* The FTP proxy is included. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 422* We incorporate here the evidence cited in support of claims 2 and 10c.	L/E
22. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process is a generic proxy	We incorporate here the evidence cited in support of claim 19. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* We incorporate here the evidence cited in support of claim 2.	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
process capable of servicing any network service which may be communicated within TCP/IP protocol, on any one of the 64K TCP/IP communications ports.		
23. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 22 wherein the kernel is modified so that it will pass to the generic proxy process any communications packet having a destination port number that indicates a port to which no custom proxy process is bound, if the generic proxy process is bound to a predefined communications port when the communications packet is received by the kernel.	We incorporate here the evidence cited in support of claim 22. A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." Policies need not be bound to a specific destination port, or service. Generic policies may be defined to cover TCP packets or UDP packets destined for any port or range of ports. http://www.fortinet.com/products/fortigate/ *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 226* We incorporate here the evidence cited in support of claim 2.	L/E
24. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 20 wherein the	We incorporate here the evidence cited in support of claim 20. FortiOS utilizes a modified Linux kernel. Linux is a Unix-like operating system.	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
gateway station is a Unix station.		
25. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the apparatus further includes programs for providing a security administrator with an interface to permit the security administrator to build a rule base for controlling communications through the gateway station.	We incorporate here the evidence cited in support of claim 19. FortiOS includes a web-based GUI and a command-line interface. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 2376* A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* We incorporate here the evidence cited in support of claims 3a, b, and 4b.	L
28. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 22 wherein the generic proxy process capable of servicing any network service which may be communicated within TCP/IP protocol, on any one of the 64K TCP/IP communications ports is a TCP proxy process.	We incorporate here the evidence cited in support of claim 22. A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." Policies need not be bound to a specific destination port, or service. Generic policies may be defined to cover TCP packets or UDP packets destined for any port or range of ports. http://www.fortinet.com/products/fortigate/ *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 226* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* We incorporate here the evidence cited in support of claim 2.	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
29. A computer system for providing a secure gateway between a private network and a potentially hostile network, comprising:	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway;	The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 1.	L/E
b) means for determining whether there is a process bound to a destination port number of an accepted communications packet;	FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231, P. 191, P. 196-197* FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported by using Application Layer Proxies. *FortiGate Version 4.0 MR2 Administration Guide P.220- 226* The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 1c.	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
c) means for establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;	If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is established (as indicated by creating an entry in the session table), else the packet is dropped. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff* FortiWeb Data Sheet, P1 The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 1d.	L/E
d) means for transparently establishing, without intervention from the source, a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and	Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet, without intervention from the source. "Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff, P. 186-187* The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 1e.	L/E
e) means for transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the	Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.* The means include the hardware and software, including FortiOS	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.	and proxies. We incorporate here the evidence cited in support of claim 1f.	
30. A computer system providing a secure gateway between a private network and a potentially hostile network as claimed in claim 29 wherein the means for determining checks to determine if a process is bound to the destination port number, and passes the packet to a generic process if a process is not bound to the destination port number, the generic process acting to establish the first and second communications sessions and to move the data between the first and second communications sessions.	A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." Policies need not be bound to a specific destination port, or service. Generic policies may be defined to cover TCP packets or UDP packets destined for any port or range of ports. http://www.fortinet.com/products/fortigate/ *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 226, 215* The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 2.	L/E
31. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 29 wherein the	We incorporate here the evidence cited in support of claim 29. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184,*	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
system further includes:	*185*	
a) means for checking a rule base to determine if the source address requires authentication; and	The list of policies includes identity-based policies which require authentication based on source address. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 925, 975-979* The means include the hardware and software, including FortiOS and proxies. We incorporate here the evidence cited in support of claim 3a.	L/E
b) means for authenticating the source by requesting a user identification and a password and referencing a database to determine if the user identification and password are valid.	FortiOS authenticates with a user identification and password checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* The means include the hardware and software, including FortiOS, data bases and proxies. We incorporate here the evidence cited in support of claim 3b.	L/E
32. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 29 wherein the system further includes:	We incorporate here the evidence cited in support of claim 29. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for referencing a rule base after the first communications session is established to determine whether the source address is permitted to access the destination address for a requested type of	A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether the communication is permitted. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.189* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.925-927* The means include the hardware and software, including FortiOS,	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
service; and	data bases and proxies. We incorporate here the evidence cited in support of claim 4a.	
b) means for cancelling the first communications session if the rule base does not include a rule to permit the source address to access the destination address for the requested type of service.	If a policy does not permit a packet, the packet is denied. The first communication session is cancelled. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923* The means include the hardware and software, including FortiOS, data bases and proxies. We incorporate here the evidence cited in support of claim 4b.	L/E
33. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 32, wherein the system further includes:	We incorporate here the evidence cited in support of claim 32. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and	Once a user successfully authenticates, the FortiGate security device creates an entry in the authentication table for the user's IP address. *FortiOS™ Handbook v2: User Authentication, P.47* Once a user authenticates using one of the defined protocols, they can access any resource permitted by the identity policy. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 925-927* There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.902* The means include the hardware and software, including FortiOS.	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	We incorporate here the evidence cited in support of claim 5a.	
b) means for referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source.	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.902* *FortiWeb Data Sheet, P. 1* The means include the hardware and software, including FortiOS. We incorporate here the evidence cited in support of claim 5b.	L/E
34. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 33 wherein the user authentication file includes a creation time variable which is set to a system time value when the user is authenticated.	We incorporate here the evidence cited in support of claim 33. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* The means include the hardware and software, including FortiOS. We incorporate here the evidence cited in support of claim 6.	E
35. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 34 wherein the system further includes:	We incorporate here the evidence cited in support of claim 34. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for updating a modification time variable of the	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
authentication file each time the user initiates a new communications session through the gateway station.	authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.902* The means include the hardware and software, including FortiOS. We incorporate here the evidence cited in support of claim 7a.	
36. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim 35 wherein the system further includes:	We incorporate here the evidence cited in support of claim 35. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for periodically checking each user authentication file to determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902* The means include the hardware and software, including FortiOS. We incorporate here the evidence cited in support of claim 8a.	E
b) means for deleting the user file from the user authentication directory if the threshold has been exceeded by each of the first and second	There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902* The means include the hardware and software, including FortiOS.	E

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
differences.	We incorporate here the evidence cited in support of claim 8b.	
37. A computer system for providing a secure gateway between a private network and potentially hostile network as claimed in claim 29 wherein the system further includes:	We incorporate here the evidence cited in support of claim 29. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) means for performing a data sensitivity check on the data associated with each packet as a step in the process of moving the data between the respective first and second communications sessions.	We incorporate here the evidence cited in support of claim 9. FortiGate security devices implement UTM components which perform data sensitivity checking while transferring data. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Chapter 6* The means include the hardware and software, including FortiOS and UTM components.	L/E
38. A computer-readable memory encoded with computer-readable instructions for providing a secure gateway between a private network and a potentially hostile network, comprising:	A FortiGate security device operating under FortiOS acts as a gateway between networks. The devices operate according to computer-readable instructions stored on computer readable memory. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) instructions for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches	The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.	L

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
the device address of the gateway;	*Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* We incorporate here the evidence cited in support of claim 1b.	
b) instructions for determining whether there is a process bound to a destination port number of an accepted communications packet;	FortiOS determines whether there is a process bound to a destination port number of an accepted communications packet by matching the packet to a policy: "When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231, P. 191, P. 196-197* FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported by using Application Layer Proxies. *FortiGate Version 4.0 MR2 Administration Guide P.220- 226* We incorporate here the evidence cited in support of claim 1c.	L/E
c) instructions for transparently establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;	If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established (as indicated by creating an entry in the session table), else the packet is dropped. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff* FortiWeb Data Sheet, P1 We incorporate here the evidence cited in support of claim 1d.	L/E
d) instructions for transparently establishing, without intervention from the source, a second communications session with a destination	Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet, without intervention from the source. "Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
address/destination port of the accepted communications packet if a first communications session is established; and	stateful inspection module uses for maintaining sessions, NAT, and other session related functions." *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 193ff, P. 186-187* We incorporate here the evidence cited in support of claim 1e.	
e) instructions for transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.	Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189 Chapter 6.* We incorporate here the evidence cited in support of claim 1f.	L/E
39. A computer readable memory as claimed in claim 38 wherein the computer readable memory comprises at least one compact disk.	This claim is infringed as described in Claim 38 if the FortiOS operating system is distributed on at least one compact disk. We incorporate here the evidence cited in support of claim 38.	L
40. A computer readable memory as claimed in claim 38 wherein the computer readable memory comprises at least one floppy diskette.	This claim is infringed as described in Claim 38 if the FortiOS operating system is distributed on at least one floppy disk. We incorporate here the evidence cited in support of claim 38.	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
41. A computer readable memory as claimed in claim 38 wherein the computer readable memory comprises at least one hard disk drive.	This claim is infringed as described in Claim 38 if the FortiOS operating system is distributed on at least one hard disk. We incorporate here the evidence cited in support of claim 38. The FortiGate unit contains a hard disk. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 117, 586, 2309*	L
42. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the step of accepting includes accepting for processing at the gateway a communications packet from the private network that (i) is addressed directly to a host on the potentially hostile network as if there were a communications path to the host, and (ii) is encapsulated with a hardware destination address that matches a device address of the gateway.	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. These packets are accepted [for processing] as long as they are encapsulated with the MAC address of the gateway. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 FortiGate Version 4.0 MR2 Administration Guide, P. 173 RFC 826, An Ethernet Address Resolution Protocol [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted]	
43. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the accepted communications packet is received at the gateway from the private network, wherein the accepted packet is addressed directly to a host on the potentially hostile network as if there were a communications path to the host and is encapsulated with the hardware destination address that matches the device address of the gateway, and wherein transparently moving data comprises passing communications packets to at least one proxy process that is configured to operate at an application layer of the gateway.	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 FortiGate Version 4.0 MR2 Administration Guide, P. 173 RFC 826, An Ethernet Address Resolution Protocol [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] Logically the client, proxy and server would be on different machines. Once the first and second sessions (between the firewall and source,	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.* [redacted] **FORTINET-NPS-SC 000066-000074** **[201:204]** [redacted] **[269:275]** [redacted] [redacted] **FORTINET-NPS-SC 000119-000124** **[50:54]** [redacted] **[250:258]** [redacted] [redacted] **FORTINET-NPS-SC 000075-000077** **[32:96]** [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] **FORTINET-NPS-SC 000140-000145** **[3997:4013]** [redacted] [redacted] **FORTINET-NPS-SC 000064-000065** **[862:867]** [redacted] [redacted] **FORTINET-NPS-SC 000015-000034** **[4:5]** [redacted] **[24:25]** [redacted] **[843:864]** [redacted]	
44. A method of providing a secure	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the subsequent communications packets received as part of the first communications session are received at the gateway from the private network, and are (i) addressed directly to a host on the potentially hostile network as if there were a communications path to the host, and (ii) encapsulated with a hardware destination address that matches a device address of the gateway.	between networks. The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 FortiGate Version 4.0 MR2 Administration Guide, P. 173 RFC 826, An Ethernet Address Resolution Protocol [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	
45. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1, further comprising:	We incorporate here the evidence cited in support of claim 1. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	
a) checking a rule base to determine if the source address requires authentication;	A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether there is a policy associated with the source address that requires authentication. The list of policies includes identity-based policies which require authentication based on source address. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, 925, 975-979* [redacted] **FORTINET-NPS-SC 000078-000082** **[5:14]** [redacted]	L/E
b) determining whether a user identification and password previously provided from the source address is sufficient to authenticate the source;	Once a user is authenticated, the FortiGate security device creates an entry in the authentication table for the user's IP address. FortiOS Handbook v2: User Authentication, P.47. Upon receiving further packets from the source address, the FortiGate security device checks against the authentication table for the user's IP address. FortiOS authenticates with a user identification and password checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* [redacted] **FORTINET-NPS-SC 000078-000082** **[15:19]** [redacted]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] **FORTINET-NPS-SC 000083-000096** **[443:444]** [redacted] **[463:464]** [redacted] **[603:615]** [redacted] [redacted] **FORTINET-NPS-SC 000098-00009** **[17:18]** [redacted] **[50]** [redacted]	
c) responsive to a determination that the previously provided user identification and password is sufficient to authenticate the source, authenticating the source without requesting a user identification and a password; and	FortiOS devices provide authentication timeout. A user does not need to provide login and password information during the timeout period. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923 FortiOS authenticates with a user identification and password checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* [redacted] **FORTINET-NPS-SC 000078-000082** **[15:19]** [redacted]	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] [redacted] FORTINET-NPS-SC 000083-000096 [443:444] [redacted] [463:464] [redacted] [603:615] [redacted] [redacted] FORTINET-NPS-SC 000098-00009 [17:18] [redacted] [50] [redacted]	
d) responsive to a determination that the previously provided user identification and password is not sufficient to authenticate the source, authenticating the source by requesting a user	There is an idle timer for the authentication. If the user session remains idle for a period of time, the session expires and the user must authenticate again. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902. FortiOS authenticates with a user identification and password if no entry exists in the authentication table that checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
identification and a password and referencing a database to determine if the user identification and password are valid.	We incorporate here the evidence cited in support of claim 45b and claim 45c.	
46. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 45, wherein the determination as to whether the previously provided user identification and password is sufficient to authenticate the source is based on an amount of time since the previously provided user identification and password was received from the source.	We incorporate here the evidence cited in support of claims 1 and 45. A FortiGate security device operating under FortiOS acts as a gateway between networks. http://www.fortinet.com/products/fortigate/; Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185 FortiOS authenticates with a user identification and password checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* [redacted] **FORTINET-NPS-SC 000078-000082** **[15:19]** [redacted] [redacted] **FORTINET-NPS-SC 000083-000096** **[443:444]** [redacted] **[463:464]** [redacted] **[603:615]** [redacted]	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] similar for: [redacted] FORTINET-NPS-SC 000098-00009 [17:18] [redacted] [50] [redacted] FortiOS devices provide authentication timeout. A user need not authenticate again during the timeout period. This authentication timeout is exemplary and applies to any Fortinet product which gives the ability to remember when a user was previously authenticated. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923* If the timeout period expires, the user must authenticate again. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902. [redacted] FORTINET-NPS-SC 000078-000082 [179:183] [redacted]	
47. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10, wherein the step of accepting from either network all TCP/IP packets includes accepting for	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted [for processing] as long as they are	L

Asserted Claim Language of U.S. Patent No. 5,623,601	**Corresponding Element in Accused Instrumentality as to Fortinet**	**Literal or Equivalent**
processing at the gateway a TCP/IP packet from the private network that (i) is addressed directly to a host on the potentially hostile network as if there were a communications path to the host, and (ii) is encapsulated with a hardware destination address that matches a device address of the gateway.	encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] Logically the client, proxy and server would be on different machines. A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol*	
48. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10, wherein the accepted TCP/IP packet is received at the gateway from the private network, wherein the accepted TCP/IP packet is addressed directly to a host on the potentially hostile network as if	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway	L/E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
there were a communications path to the host and is encapsulated with the hardware destination address that matches the device address of the gateway, and wherein transparently moving data comprises passing communications packets to a proxy process which operates at an application layer of the gateway to extract the data from the each subsequent TCP/IP packet and then pass the extracted data between the first and second communications sessions.	such as by using ARP. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol* Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.* [redacted] **FORTINET-NPS-SC 000066-000074** **[201:204]** [redacted] **[269:275]** [redacted] [redacted] **FORTINET-NPS-SC 000119-000124** **[50:54]** [redacted] **[250:258]** [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] FORTINET-NPS-SC 000075-000077 [32:96] [redacted] [redacted] FORTINET-NPS-SC 000140-000145 [3997:4013] [redacted] [redacted] FORTINET-NPS-SC 000064-000065 [862:867] [redacted] [redacted] FORTINET-NPS-SC 000015-000034 [4:5] [redacted] [24:25] [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[843:864] [redacted]	
49. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10, wherein the subsequent communications packets received as part of the first communications session are received at the gateway from the private network, and are (i) addressed directly to a host on the potentially hostile network as if there were a communications path to the host, and (ii) encapsulated with a hardware destination address that matches a device address of the gateway.	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185* *FortiGate Version 4.0 MR2 Administration Guide, P. 173* *RFC 826, An Ethernet Address Resolution Protocol*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
50. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10, further comprising:	We incorporate here the evidence cited in support of claim 10. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185*	
a) checking a rule base to determine if the source requires authentication;	A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether there is a policy associated with the source address that requires authentication. The list of policies includes identity-based policies which require authentication based on source address. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189 and 925* We incorporate here the evidence cited in support of claim 45a.	E
b) checking an authentication directory to determine if an authentication file exists for the source in an instance where the source requires authentication; and	Once a user successfully authenticates, the FortiGate security device creates an entry in the authentication table for the user's IP address. Upon receiving further packets from the source address, the FortiGate security device checks against the authentication table for the user's IP address. This authentication table (and check to see if any change has occurred) is exemplary and applies to any Fortinet product which gives the ability to remember when a source address was previously authenticated. *FortiOS™ Handbook v2: User Authentication, P.47* [redacted] **FORTINET-NPS-SC 000078-000082** **[151:156]** [redacted]	E
c) responsive to a determination that an authentication file for	FortiOS devices provide authentication timeout. A user does not need to provide login and password information during the timeout	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
the source exists and if the source requires authentication, authenticating the source without requesting a user identification and a password; and	period. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.923 FortiOS authenticates with a user identification and password if no entry exists in the authentication table that checked against a local or remote database. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915* We incorporate here the evidence cited in support of claim 45c.	
d) if the source requires authentication and an authentication file for the source cannot be located, authenticating the source by requesting a user identification and a password and referencing a user identification database to determine if the user identification and password are valid.	We incorporate here the evidence cited in support of claim 45d. There is an idle timer for the authentication. If the user session remains idle for a period of time, the session expires and the user must authenticate again. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902. FortiOS authenticates by checking a user identification and password against a local or remote database. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 915.	E
51. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19, wherein the operating system is configured such that the operating system will accept for processing by the operating system a communications packet from the private network that is addressed to a host on	We incorporate here the evidence cited in support of claim 19. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
the potentially hostile network as if there were a communications path from the private network to the host, and that is encapsulated with the hardware destination address that matches the device address of the gateway station on the private network.	there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 FortiGate Version 4.0 MR2 Administration Guide, P. 173 RFC 826, An Ethernet Address Resolution Protocol [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	
52. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19, wherein the at least one proxy process is configured to operate at the application layer to transparently pass the data portion of packets between the first and second communications sessions.	We incorporate here the evidence cited in support of claim 19. FortiGate security device provides predefined services for common application layer protocols using standard port numbers (or range of port numbers). Additional proxy based services are supported by using Application Layer Proxies. FortiGate Version 4.0 MR2 Administration Guide P.220- 226 [redacted] **FORTINET-NPS-SC 000039-000043** **[41:45]** [redacted]	L/E
53. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19, wherein the	We incorporate here the evidence cited in support of claim 19. A FortiGate security device operating under FortiOS acts as a gateway between networks. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184,*	L

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
initial data packet is a communications packet received by the gateway from the private network and accepted for processing by the operating system, that is addressed to a host on the potentially hostile network as if there were a communications path from the private network to the host, and that is encapsulated with the hardware destination address that matches the device address of the gateway station on the private network.	*185* [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted] A FortiGate security device operating under FortiOS is configured as a gateway so that end devices use the destination IP address as if there were a communications path to the host but encapsulating the packets with the MAC address of a device address of the gateway such as by using ARP. Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185 FortiGate Version 4.0 MR2 Administration Guide, P. 173 RFC 826, An Ethernet Address Resolution Protocol [redacted] **FORTINET-NPS-SC 000066-000074** **[378:381]** [redacted]	
55. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 25, wherein the rule base determines if the source address requires authentication based on a user identification and a password that matches a user identification and password	We incorporate here the evidence cited in support of claim 25. A FortiGate security device operating under FortiOS acts as a gateway between networks. FortiOS devices provide authentication timeout. A user need not authenticate again during the timeout period. This authentication table (and check to see if any change has occurred) is exemplary and applies to any Fortinet product which gives the ability to remember when a source address was previously authenticated. *http://www.fortinet.com/products/fortigate/* *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185* [redacted] **FORTINET-NPS-SC 000078-000082** **[179:183]**	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
maintained in a user authentication file which contains the source address of the authenticated user in a user authentication directory, and wherein the authentication file is used to determine whether a source address has been authenticated each time a new communications session is initiated, whereby the gateway is completely transparent to an authenticated source.	[redacted] [redacted] [redacted] **FORTINET-NPS-SC 000078-000082** **[151:156]** [redacted] [redacted] [redacted] **FORTINET-NPS-SC 000107-00108** **[53:75]** [redacted] [redacted] [redacted] [redacted] [redacted] **FORTINET-NPS-SC 000100-00106** **[130:269]** [redacted] [redacted] [redacted] We incorporate here the evidence cited in support of claim 1d.	
56. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 55, wherein a modification time	We incorporate here the evidence cited in support of claim 55. There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 899,902,* [redacted] **FORTINET-NPS-SC 000107-00108** **[741:773]**	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
variable of the authentication file is updated each time the user initiates a new communications session through the gateway station and wherein the user file is deleted from the user authentication directory if one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold.	[redacted] [redacted] [redacted] [redacted] FORTINET-NPS-SC 000107-00108 [775:789] [redacted] There is an idle timer for the authentication. If the user session remains idle for that long, the session expires and the user must authenticate again. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P.899, 902* [redacted] FORTINET-NPS-SC 000078-000082 [15:21] [redacted] [181:183] [redacted]	
57. Apparatus for providing a secure	We incorporate here the evidence cited in support of claim 19. A FortiGate security device operating under FortiOS acts as a	E

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
gateway for data changes between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process is further adapted to perform a data sensitivity check is on the data associated with each packet while transparently passing the data portion of the each packet.	gateway between networks. http://www.fortinet.com/products/fortigate/ Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185 FortiGate security devices implement UTM components which perform data sensitivity checking while transferring data. The below is an exemplary data sensitivity check and applies to all data sensitivity checks done in Fortinet source code. *Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Chapter 6* [redacted] **FORTINET-NPS-SC 000125-000126** **[5:8]** [redacted] [redacted] **FORTINET-NPS-SC 000127** **[8:11]** [redacted] [redacted] **FORTINET-NPS-SC 000128** **[11:35]** [redacted] [redacted] **FORTINET-NPS-SC 000129-000130** **[11]** [redacted]	

Asserted Claim Language of U.S. Patent No. 5,623,601	Corresponding Element in Accused Instrumentality as to Fortinet	Literal or Equivalent
	[redacted] **FORTINET-NPS-SC 000131** **[8:13]** [redacted] [redacted] **FORTINET-NPS-SC 000044-000045** **[10:18]** [redacted] [redacted] **http://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol** The Internet Content Adaptation Protocol (ICAP) is a lightweight HTTP-like protocol specified in RFC 507 which is used to extend transparent proxy servers, thereby freeing up resources and standardizing the way in which new features are implemented. ICAP is generally used to implement virus scanning and content filters (including censorware) in transparent HTTP proxy caches.	